CLAIMS

1. Apparatus for processing data, said apparatus comprising:

a processor responsive to a plurality of different program instructions to perform respective processing operations each requiring a number of processing cycles to complete, said plurality of program instructions including at least one variable timing instruction requiring between a minimum number of cycles and a maximum number of cycles to complete, wherein

said processor is operable in a variable timing mode in which said at least one variable timing instruction is permitted to take a variable number of processing cycles to complete; and

said processor is operable in a fixed timing mode in which said at least one of variable timing instruction is forced to take said maximum number of cycles to complete.

2. Apparatus as claimed in claim 1, wherein said at least one variable timing instruction includes a conditional instruction, said processor being operable in said variable timing mode to suppress execution of said conditional instruction in dependence upon one or more condition codes set in response to execution of one or more previously executed program instructions and said processor being operable in said fixed timing mode to complete said conditional instruction in a fixed number of processing cycles irrespective of said one or more condition codes set in response to execution of one or more previously executed program instructions.

3. Apparatus as claimed in claim 2, wherein when executing said conditional instruction in said fixed timing mode, if said conditional codes are such that execution of said conditional instruction would have been suppressed in said variable timing mode, then said conditional instruction is blocked for making any change effecting subsequent data processing operations.

4. Apparatus as claimed in claim 3, wherein if said conditional instruction is a conditional branch instruction, then when executing said conditional branch instruction in said fixed timing mode, if said conditional codes are such that execution of said conditional branch instruction would have been suppressed in said variable

timing mode, then said conditional branch instruction is forced to perform a branch to a next instruction irrespective of any branch target specified in said conditional branch instruction.

5. Apparatus as claimed in claim 3, wherein if said conditional instruction is a conditional data manipulating instruction, then when executing said conditional data manipulating instruction in said fixed timing mode, if said conditional codes are such that execution of said conditional data manipulating instruction would have been suppressed in said variable timing mode, then said conditional data manipulating instruction is prevented from writing a result to any normal result destination of said conditional data manipulating instruction.

6. Apparatus as claimed in claim 5, wherein if writing of said result to any normal destination is prevented, then said result is instead written to at least one dummy destination.

7. Apparatus as claimed in claim 6, wherein said at least one dummy destination include a dummy processor register.

8. Apparatus as claimed in claim 1, wherein said at least one variable timing instruction includes an instruction capable of early termination in dependence upon one or more data values being processed, said processor being operable in said variable timing mode to permit early termination and said processor being operable in said fixed timing mode to prevent early termination.

9. Apparatus as claimed in claim 8, wherein said instruction capable of early termination is one of:

a multicycle multiply instruction;

a multicycle divide instruction;

a multicycle add instruction; and

a mutlicycle subtract instruction.

10. Apparatus as claimed in any one of the preceding claims, wherein said processor adopts said variable timing mode or said fixed timing mode in dependence upon a programmable mode controlling parameter.

11. Apparatus as claimed in claim 10, wherein said programmable mode controlling parameter is stored within a system configuration register.

12. Apparatus as claimed in any one of the preceding claims, wherein said processor is switched into said fixed timing mode so as to disguise a program execution path.

13. A method of processing data using a processor responsive to a plurality of different program instructions to perform respective processing operations each requiring a number of processing cycles to complete, said plurality of program instructions including at least one variable timing instruction requiring between a minimum number of cycles and a maximum number of cycles to complete, said method comprising the steps of:

operating said processor in a variable timing mode in which said at least one variable timing instruction is permitted to take a variable number of processing cycles to complete; and

operating said processor in a fixed timing mode in which said at least one of variable timing instruction is forced to take said maximum number of cycles to complete.

14. A method as claimed in claim 13, wherein said at least one variable timing instruction includes a conditional instruction and further comprising operating said processor in said variable timing mode to suppress execution of said conditional instruction in dependence upon one or more condition codes set in response to execution of one or more previously executed program instructions and said processor being operable in said fixed timing mode to complete said conditional instruction in a fixed number of processing cycles irrespective of said one or more condition codes set in response to execution of one or more previously executed program instructions.

15. A method as claimed in claim 14, wherein when executing said conditional instruction in said fixed timing mode, if said conditional codes are such that execution of said conditional instruction would have been suppressed in said variable timing mode, then said conditional instruction is blocked for making any change effecting subsequent data processing operations.

16. A method as claimed in claim 15, wherein if said conditional instruction is a conditional branch instruction, then when executing said conditional branch instruction in said fixed timing mode, if said conditional codes are such that execution of said conditional branch instruction would have been suppressed in said variable timing mode, then said conditional branch instruction is forced to perform a branch to a next instruction irrespective of any branch target specified in said conditional branch instruction.

17. A method as claimed in claim 15, wherein if said conditional instruction is a conditional data manipulating instruction, then when executing said conditional data manipulating instruction in said fixed timing mode, if said conditional codes are such that execution of said conditional data manipulating instruction would have been suppressed in said variable timing mode, then said conditional data manipulating instruction is prevented from writing a result to any normal result destination of said conditional data manipulating instruction.

18. A method as claimed in claim 17, wherein if writing of said result to any normal destination is prevented, then said result is instead written to at least one dummy destination.

19. A method as claimed in claim 18, wherein said at least one dummy destination include a dummy processor register.

20. A method as claimed in claim 13, wherein said at least one variable timing instruction includes an instruction capable of early termination in dependence upon one or more data values being processed and further comprising operating said processor in said variable timing mode to permit early termination and said processor being operable in said fixed timing mode to prevent early termination.

21. A method as claimed in claim 20, wherein said instruction capable of early termination is one of:

a multicycle multiply instruction;

a multicycle divide instruction;

a multicycle add instruction; and

a mutlicycle substract instruction.

22. A method as claimed in any one of claims 13 to 21, wherein said processor adopts said variable timing mode or said fixed timing mode in dependence upon a programmable mode controlling parameter.

23. A method as claimed in claim 22, wherein said programmable mode controlling parameter is stored within a system configuration register.

24. A method as claimed in any one of claims 13 to 23, wherein said processor is switched into said fixed timing mode so as to disguise a program execution path.